Mixed PUF-TRNG Circuit using Body Biasing in FD-SOI

Jean-Luc Danger Risa Yashiro Tarik Graba
Yves Mathieu Kazuo Sakiyama Sylvain Guilley

April 9, 2018

Abstract

It is known that an SR-latch can be regarded as primitive to build either a True Random Number Generation (TRNG) or a Physically Unclonable Function (PUF). Indeed, when the SR inputs of the latch are tied together and go from an unknown state (i.e. S=R=1) to a memory state (i.e. S=R=0), the behaviour depends on the balance between the NAND or NOR gates composing the latch. With the process mismatch, there is a great chance that the latch converges towards the same state, thus creating a PUF equivalent to a SRAM-PUF or latch-PUF. However, if the latch is well-balanced, it can enter a metastable state and converges to a stable state depending on the input noise, thus making a TRNG. In order to make sure some latches are able to behave like a TRNG, and some like a PUF, we consider a set of latches driven by the same SR signal. A test-chip in 28nm FD-SOI technology has been designed with 1024 latches in order to analyze the behavior. This technology enables an easy change of the performances by using body biasing. Using a different and adjustable bias for the two NOR gates composing the SR-latch, it becomes possible to get a mixed PUF-TRNG circuit which provides high reliability for the PUF and High speed for the TRNG.